AFRL-IF-RS-TR-2001-45
Final Technical Report
April 2001

EFFECTS-BASED CYBERCOA OPTIMIZATION TECHNOLOGY & EXPERIMENTS: PREDICTING THE IMPACT OF DISRUPTIONS TO BMC3 WORKFLOW

ALPHATECH, Inc.

Sponsored by
Defense Advanced Research Projects Agency
DARPA Order No. AOJ353/02 & 03

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2001-45 has been reviewed and is approved for publication.

APPROVED:

PETER J. ROCCI
Project Engineer

FOR THE DIRECTOR:

JAMES A. COLLINS, Acting Chief
Information Technology Division
Information Directorate

If your address has changed or if you wish to be removed from the Air Force Research Laboratory Rome Research Site mailing list, or if the addressee is no longer employed by your organization, please notify AFRL/IFTD, 525 Brooks Road, Rome, NY 13441-4505. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

EFFECTS-BASED CYBERCOA OPTIMIZATION TECHNOLOGY & EXPERIMENTS: PREDICTING THE IMPACT OF DISRUPTIONS TO BMC3 WORKFLOW

John Shaw and Leonard Lublin

Contractor: Alphatech, Inc.
Contract Number: F30602-00-C-0184
Effective Date of Contract: 19 June 00
Contract Expiration Date: 28 February 2001
Short Title of Work: Effects-Based CyberCOA Optimization Technology & Experiments: Predicting the Impact of Disruptions to BMC3 Workflow
Period of Work Covered: Jun 00 - Feb 01

Principal Investigator: John Shaw & Leonard Lublin
Phone: (617) 273-3388
AFRL Project Engineer: Peter J. Rocci
Phone: (315) 330-4654

This research was supported by the Defense Advanced Research Projects Agency of the Department of Defense and was monitored by Peter J. Rocci, AFRL/IFTD, 525 Brooks Road, Rome, NY.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	APRIL 2001	Final Jun 00 - Feb 01

4. TITLE AND SUBTITLE
EFFECTS-BASED CYBERCOA OPTIMIZATION TECHNOLOGY & EXPERIMENTS: PREDICTING THE IMPACT OF DISRUPTIONS TO BMC3 WORKFLOW

5. FUNDING NUMBERS
C - F30602-00-C-0184
PE - 62301E
PR - J353
TA - 33
WU - B1

6. AUTHOR(S)
John Shaw and Leonard Lublin

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
ALPHATECH, Inc.
50 Mall Road
Burlington MA 01803-4562

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Advanced Research Projects Agency
3701 North Fairfax Drive
Arlington VA 22203

Air Force Research Laboratory/IFTD
525 Brooks Road
Rome NY 13441-4505

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2001-45

11. SUPPLEMENTARY NOTES
Air Force Research Laboratory Project Engineer: Peter J. Rocci/IFTD/(315) 330-4654

12a. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*
This report discusses the feasibility of developing advanced, closed-loop, optimal control technology, which will allow a cyber-commander to formulate and select Courses of Action (COAs) that balance security objectives against mission effectiveness. The initial formulation includes a plant model (incorporating the cyber-network, assignment of processes and information flows to elements of the cyber-network, and a mission model) with a unified objective function incorporating the commander's goals of both Information Assurance & Survivability and traditional military missions.

14. SUBJECT TERMS
Courses of Action (COAs), Cyber-Network, Information Assurance

15. NUMBER OF PAGES
36

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Table of Contents

List of Figures

SECTION 1
INTRODUCTION

1.1 THE PROBLEM

A fundamental challenge for modern Battle Management/Command, Control, and Communications (BMC3) systems is to withstand attacks against their constituent computer and communication subsystems. Measures introduced by System Administrators to safeguard or respond to a "cyber attack" will vary with the type of attack, of course, but almost all measures will disrupt the processing flow within the BMC3 system in some manner. Encryption, for instance, will invariably introduce processing and communication delays within the BMC3 system. Re-locating a database server will both introduce delays and interrupt processing. Every BMC3 system is in a race against time, and disruptions in its processing flow may very well cause the system to lose the race.

System Administrators disrupt BMC3 processing flows with startling regularity even under benign conditions when their systems are not under attack, and the consequences are often dire. Two examples from Joint Experiment Force Exercise (JEFX) 2000 illustrate the impact of even "modest" disruption on time-critical BMC3 processing.

In the first example, the Combined Air Operations Center (CAOC) at Hurlburt Field was performing Time-Critical Targeting with the TCT cell at Nellis AFB. System Administrators at Hurlburt discovered a minor configuration problem, and attempted to fix the problem with a system upgrade. The upgrade, however, caused a loss of synchronization in the data appearing on the Common Operational Pictures (COPs) at Hurlburt and Nellis. With this loss of synchronicity the CAOC at Hurlburt was no longer able to see targets nominated for engagement by the TCT cell at Nellis. Confusion quickly settled in: the CAOC observed strike aircraft diverted (to engage TCTs) without knowing why. CAOC operators assumed that the air plan had gone awry, and suspended missions in order to straighten out the situation.

The second example involved planned system outage for maintenance at the CAOC. The directors for Current Operations and for System Administration agreed to a plan to take the system down a) after

7PM, and b) after air planners had finished building the strike package. The System Administration staff were instructed on the first condition, but not the second. The system was taken down for maintenance at 7 PM before the air plan was completed, and several hours of data were lost.

In both cases, the System Administrators did not know that their BMC3 systems were in the midst of critical workflows that simply could not be interrupted. This point is vitally important as we look beyond the relatively benign conditions in those circumstances to the challenges of responding to cyber attacks. System Administrators cannot respond intelligently to a cyber attack if they are unable to anticipate how disruptions in the ongoing workflow will affect the mission.

1.2 Research Objectives

The objective of the EBCOTE project is to develop technology based on advanced, closed-loop, optimal control, which will allow a cyber-commander to formulate and select courses of action (COAs) that balance security objectives against mission effectiveness. This document reports our progress towards developing that technology accomplished under a six-month feasibility study.

We made an important discovery early in this feasibility study: there is no efficient method to determine in real-time how a cyber-COA will impact the ongoing workflow in a BMC3 system. More to the point, it is difficult to determine the mission impact of a disruption in the BMC3 workflow, be it in response to a cyber-COA or any other action by System Administrators.

During our feasibility study, therefore, we set out to develop an efficient method to predict how disruptions in the processing flow within a BMC3 system affect mission performance. We developed an analysis method based on perturbation analysis. Specifically, we developed a mathematical foundation for analyzing perturbations around a nominal BMC3 workflow to answer the following questions:

1. What are the consequences if we retard the workflow processing within a BMC3 system?;
2. What are the consequences if we interrupt the workflow processing (i.e., halt the processing and restore at a later time)?; and

3. What are the consequences if we halt the workflow processing altogether?

We approximate the nominal workflow processing conducted by a BMC3 system using a Markov model, and from there develop important sensitivity metrics from Optimal Control Theory, most notably 'cost-to-go,' and 'co-state.'

This Technical Report presents this analysis method. It is organized into five sections, this introduction being the first. In the next section we develop a general workflow model to describe processing activities within a general BMC3 system. In Section 3 we develop the Markov model approximation to describe nominal workflow processing, and derive key sensitivity metrics to measure the effects of perturbations around that nominal flow. In Section 4 we present numerical results from the analysis of a missile defense BMC3 system. We close this report in Section 5 with directions for future research.

SECTION 2
MODELLING BMC3 WORKFLOW PROCESSING

2.1 INTRODUCTION

BMC3 systems typically perform many coordinated activities in order to carry out a mission. For instance, if the mission is to prosecute Time-Critical Targets, then the high-level activities might be to manage surveillance, nominate targets for prosecution, maintain track and combat ID on nominated targets, assign weapons to targets, monitor engagements in progress, and assess the engagement results. People and machines perform these activities, each fulfilling specified roles and responsibilities, and all in accordance with established rules and procedures. These activities are typically triggered by events external to the BMC3 system (e.g., the detection of an enemy vehicle, the arrival of an Alert Order from Higher Authority), and culminate in orders and directives issued to external organizations and units.

The operational aspects of a BMC3 system—the sequence of tasks and who performs them, the information flow to support the tasks, and the tracking and reporting mechanisms that measure and control them—describe a workflow. We introduce here important terms from Workflow [1] that we shall use throughout this paper:

- Task: a unit of work that is to be performed (i.e., completed) by the workflow system; also known as a *work item*. A task may represent a specific thing to be accomplished (e.g., add an air mission to the Air Tasking Order), or it may represent a collection of things to be accomplished (e.g., assemble the Air Tasking Order). For clarity throughout this paper we use 'task' to represent the former, and 'mission' to represent the latter.
- Completion State: a specific and measurable degree of completion of a task.
- Activity: an action that acts on a task, moving it from one Completion State to another. Preferably, the direction of movement is toward a more advanced Completion State.
- Activity List: specific activities that can work on a Task when it has achieved a specific Completion State.

- Work List: specific Tasks that are awaiting processing by a specific Activity.
- Potential Work List: Completion States that can be processed by a specific Activity; tasks in the activity's Work List occupy those Completion States.
- Resource: the specific entities that carry out activities. Activities are performed by people and by machines in accordance with rules and procedures. We use the term 'cyber-resource' to refer to machines generally.
- Priority: the value assigned to the completion of a task.
- Deadline: a desired time for completing a task. A task has a 'hard' deadline if the system receives no value if the task is not complete by that time. Similarly, a task has a 'soft' deadline if the completion value diminishes for tasks completed past the deadline.

2.2 Work Completion: A Probabilistic View

Let us consider a task that has achieved a specific Completion State at a specific point in time[1]. The question before us is this: what Completion State will that task achieve at a future point in time? Random events will affect the processing on this task from this point in time on out, and we cannot predict with absolute certainty which Completion State that task will achieve. At best, therefore, we can only anticipate that the task has some probability distribution of achieving different completion states at that future point in time.

Let $\rho_{i,j,t}$ denote the probability that Task i has achieved Completion State j at time t. Let $P_{i,t}$ denote the probability distribution of Completion States that Task i can occupy at time t:

---

[1] Time can mean several things here. It can be referenced against an absolute wall clock. This is a convenient reference if the BMC3 mission of interest is episodic in nature with many tasks appearing all at once. Responding to a missile attack is one such example. Time can also be relative to the time a task enters the system. This is a convenient reference if the BMC3 mission involves numerous recurring tasks that enter the system at vastly different times. Providing Air-to-Ground support is an example of the latter. We derive the equations herein with the first meaning in mind, and observe that only trivial changes in notation are needed to accommodate the second meaning.

$$P_{i,t} = \begin{bmatrix} \rho_{i,1,t} \\ \rho_{i,2,t} \\ \cdot \\ \\ \cdot \\ \rho_{i,J,t} \end{bmatrix} \qquad (1)$$

where J represents the number of distinct Completion States that a task can achieve within the BMC3 workflow. We call $P_{i,t}$ the Completion Probability Distribution for Task i. Let Π_t denote the joint probability distribution of Completion States for all tasks that are within the BMC3 workflow at time t. We refer to Π_t as the *Workflow Completion Probability Distribution* for the BMC3 system.

Workflow completion rates can be determined using workflow analysis models [2-5], and there are a number of simulation tools designed specifically for this purpose [e.g., COSA FlowModeller, Woflan, and SES Workbench]. Our intention here is not to propose yet another model for computing workflow completion rates. Rather, our objective is to develop useful sensitivity metrics for changes in workflow completion rates that have been determined by such a model. For our purpose, then, it is sufficient to observe that the Workflow Completion Probability Distribution at a specific time is a function of both the Workflow Completion Probability Distribution at a previous time, and the status of the Resources that can perform activities on the tasks within the BMC3 system. We express the change in the Workflow Completion Probability Distribution over time using the following equation:

$$\Pi_{t+1} = \lambda[\Pi_t, R_t] \qquad (2)$$

where R_t denotes the status of the BMC3 resources (both human and machine) at time t.

2.3 The Value of Work Completed

Work completed by the BMC3 system provides value to the military mission. We introduce a general function $\psi(.)$ to compute the expected value of tasks completed at any point in time. This function takes as its argument the Workflow Completion Probability Distribution for the time in question and returns

the value provided to the military mission. We make no assumptions about this function other than it takes into account both hard and soft task completion deadlines.

Every military mission typically has a completion point, and it is there that we roll-up the expected value of tasks successfully completed into Mission Effectiveness. If we denote the mission completion time by T, then the expected Mission Effectiveness, ψ, is simply:

$$\psi = \psi(\Pi_T) \tag{3}$$

2.4 Determining the Impact of a Perturbation

Suppose we introduce a temporary perturbation to the nominal workflow within a BMC3 system at some time t. Perturbations can arise for a number of reasons, but the ones that concern us here are changes in the status of BMC3 resources (e.g., due to a cyber-attack) at the time in question. We can use Equations 2 and 3 to relate a workflow perturbation to a change in expected Mission Effectiveness. Conceptually, the relationship is as follows:

$$\frac{\partial \psi}{\partial R_t} = \frac{\partial \psi(\Pi_T)}{\partial \Pi_T} \cdot \frac{\partial \Pi_T}{\partial \Pi_{T-1}} \cdots\cdots \frac{\partial \Pi_{t+2}}{\partial \Pi_{t+1}} \frac{\partial \Pi_{t+1}}{\partial \lambda[\Pi_t, R_t]} \frac{\partial \lambda[\Pi_t, R_t]}{\partial R_t} \tag{4}$$

or, collapsing terms:

$$\frac{\partial \psi}{\partial R_t} = \frac{\partial \psi(\Pi_T)}{\partial \Pi_{t+1}} \frac{\partial \Pi_{t+1}}{\partial \lambda[\Pi_t, R_t]} \frac{\partial \lambda[\Pi_t, R_t]}{\partial R_t} \tag{5}$$

Equation 5 expresses the following intuitive point: a change in mission effectiveness due to a temporary change in BMC3 Resource status ($\partial\psi/\partial R_t$) is achieved through the combination of a near-term effect and a downstream effect. The near-term effect is the temporary change in task completion rates due to the temporary perturbation in Resource status, leading to a change in the Workflow Completion Probability Distribution achieved at the next time step. The near-term effect is captured in the last two terms in the right-hand side of Equation 5-3 $\left(\frac{\partial \Pi_{t+1}}{\partial \lambda[\Pi_t, R_t]} \frac{\partial \lambda[\Pi_t, R_t]}{\partial R_t} \right)$. The downstream effect is the change in

mission effectiveness that results as a consequence of a change in the Workflow Completion Probability Distribution. This effect is captured in the first term in the right-hand side of Equation 5-3 $\left(\frac{\partial\psi(\Pi_T)}{\partial\Pi_{t+1}}\right)$.

This latter term is known as the *co-state* [6]. It is the change in the expected Mission Effectiveness that will ultimately transpire if task Completion States are marginally perturbed from their nominal values at the time in question (t). The second right-hand side term in Equation 5 captures how a change in activity completion rates at one point in time changes task Completion States at the next point in time. The combination of this term and the co-state captures how a perturbation in activity completion ultimately leads to a change in Mission Effectiveness.

The final right-hand side term in Equation 5 relates a perturbation in BMC3 resource status to activity completion rates. Intuitively, it relates throughput to system resources, and this is the relationship that is captured in workflow analysis models.

2.5 Co-State Values, Slack, and Critical Paths

The value of the co-state for a Completion State is intimately tied to the time required to complete a task, and the time available to complete a task. Suppose a task is in a Completion State at a point in time where the expected time required to complete the task is much less than the time available to complete the task. The task, in short, is not on a critical path. In this situation there is little consequence if the task were to be in a slightly more advanced Completion State or a slightly less advanced Completion State: the system has plenty of time to complete the processing of the task either way. The co-state for this Completion State, therefore, will be negligible, and possibly zero.

Consider the other extreme: the task is in a Completion State where the expected time required to complete the task is much larger than the time available to complete the task. This may be a critical condition for the task, but from a workflow perspective the task is no longer on the critical path. Again, there is little consequence if the task were to be in a slightly more advanced Completion State or a slightly

less advanced Completion State, although for different reasons than before: the system simply has no time to complete the processing of the task. As before, the co-state for this Completion State will be negligible.

Finally, consider a condition midway between these two extremes: the task is in a Completion State where the expected time required to complete the task is comparable to the time available to complete the task. That task is on, or is approaching, a critical path. In this situation there is vast difference between being in a slightly more advanced Completion State or a slightly less advanced Completion State. The co-state will reflect this difference, and possibly be quite appreciable.

In short, the value of the co-state for a Completion State reflects whether or not the Completion State is on a critical processing path. The co-state will be negligible if the Completion State is not on a critical path. The value of the co-state rises as the Completion State approaches the critical path, and peaks roughly at a point in time when the expected time required to complete the task from that Completion State is equal to the time available.

SECTION 3
A MARKOV MODEL APPROXIMATION

Suppose we simplify Equation 2 by assuming that tasks have identical completion rates and are largely de-coupled from each other. We replace Equation 2 with the following Markov model:

$$P_{i,t+1} = \lambda_t P_{i,t} \qquad i=1,.....I \qquad (6)$$

where λ_t is a J-by-J matrix of completion state transition probabilities. These transition probabilities are a function of the status of the BMC3 resources at time t. For clarity we do not explicitly express λ_t as a function of the BMC3 resources, but recognize the dependency implicitly.

We also simplify Equation 3 to compute the Mission Effectiveness of work completed:

$$\psi = \sum_{i=1}^{I} \psi_i(P_{i,T}) \qquad (7)$$

where $\psi_i(.)$ is a function for determining the value of Completion States for task i at the mission deadline T.

3.1 Computing Cost-To-Go

The concept of co-state presented in Section 2.3 is a powerful sensitivity metric, and we would like to use the Markov model to our advantage when computing this measure. We introduce here another important concept from optimal control just for this purpose: cost-to-go. Cost-to-go is the expected mission value that will be achieved if a task is in a specific state of completion at a specific time.

If task i has achieved Completion State j by the mission deadline, then the cost-to-go, $C_{i,j,T}$, is simply $\psi(e_j)$, where e_j is the unit vector with 1 in the j^{th} position. Let $C_{i,T}$ denote the cost-to-go vector for task i at time T:

$$C_{i,T} = \begin{bmatrix} C_{i,1,T} \\ C_{i,2,T} \\ \cdot \\ \cdot \\ C_{i,J,T} \end{bmatrix} = \begin{bmatrix} \psi_i(e_1) \\ \psi_i(e_2) \\ \cdot \\ \cdot \\ \psi_i(e_J) \end{bmatrix} \qquad (8)$$

We now work backwards in time and consider the time step just prior to T. Suppose task i is in Completion State j by T-1. Its cost-to-go from that state is determined by the following equation:

$$C_{i,j,T-1} = \lambda^{j}_{T-1} C_{i,T} \qquad (9)$$

where λ^{j}_{T-1} denotes the j^{th} row of the state transition probability matrix λ_{T-1}. The cost-to-go vector for task i at time T-1 is determined by the following equation:

$$C_{i,T-1} = \lambda_{T-1} C_{i,T} \qquad (10)$$

The cost-to-go vector for task i at any arbitrary time, therefore, can be computed using the following recursive formula:

$$C_{i,t} = \lambda_{t} C_{i,t+1} \qquad (11)$$

3.2 Computing Approximate Co-States

We can divide the Completion States that can be reached from a specific Completion State into two sets: those whose cost-to-go is at least as good as the cost-to-go from the Completion State in question, and those whose cost-to-go is not as good. We denote those sets for task i, in Completion State j at time t as $D_{i,j,t}$ and $U_{i,j,t}$, respectively.

We seek a way to measure the change in the cost-to-go from a specific Completion State that will occur if the BMC^3 system is slightly more successful arranging favorable state transitions from that state. This is similar to, but not quite the same as, co-state introduced earlier in Section 2.3, and we adopt the term *approximate co-state* for this measure. We first derive the approximate co-state for a Completion State that has a single desirable and a single undesirable Completion State, and then derive the expression for approximate co-state for the more general case.

Let us suppose that a task in Completion State j at time t can reach one of only two Completion States in the next time period: k and m. Assume, with no loss in generality, that k is the desirable Completion State and m is the undesirable Completion State. Suppose the nominal transition probabilities

to those two states are α and (1 - α), respectively. The cost-to-go from Completion state j at time t, therefore, is:

$$C_{i,j,t} = \alpha\, C_{i,k,t+1} + (1-\alpha) C_{i,m,t+1} \quad (12)$$

Suppose that the BMC^3 system can increase by $\in$ the probability that the task will go to the desirable Completion State k. From inspection, the net change in the cost-to-go from state i is:

$$\Delta C_{i,j,t} = \in \left(C_{i,k,t+1} - C_{i,m,t+1}\right) \quad (13)$$

leading to the following expression for the approximate co-state $\Gamma_{i,j,t}$:

$$\Gamma_{i,j,t} = \frac{\partial C_{i,j,t}}{\partial \alpha} = \lim_{\in \to 0} \frac{\Delta C_{i,j,t}}{\in} = \left(C_{i,k,t+1} - C_{i,m,t+1}\right) \quad (14)$$

In general, a task may be able to reach a large number of Completion States from a specific Completion State. Extending Equation 14 to the general case is trivial:

$$\Gamma_{i,j,t} = \sum_{k \in D_{i,j,t}} C_{i,k,t+1} - \sum_{m \in U_{i,j,t}} C_{i,m,t+1} \quad (15)$$

3.3 Determining the Impact of Instantaneous Disruptions to Specific BMC3 Activities

What is the impact of a short-lived incremental disruption to a specific BMC3 activity? Consider an activity ϕ that works on tasks that are in specific Completion States. Those Completion States define the Potential Work List for that activity, and we denote this list by W_ϕ. A short-lived incremental disruption in activity ϕ will lead to an incremental change in the completion status for the Completion States in W_ϕ. We already know how to evaluate the latter impact: this is simply the approximate co-state. The Instantaneous Disruption Impact on Mission Effectiveness (IDIME) for activity ϕ at time t, therefore, is:

$$IDIME_{\phi,t} = \sum_{i=1}^{I} \sum_{j \in W_\phi} P_{i,j,t} \Gamma_{i,j,t} \quad (16)$$

The IDIME metric is the product of two components: the co-states for the Completion States in the Potential Work List, and the number of tasks that are in those Completion States. The IDIME profile for an

activity may peak at several times, due either to a large volume of tasks in the Work List, to a peak in co-states, or to a combination of these two factors.

3.4 Determining the Impact of Persistent Disruptions to Specific BMC3 Activities

What is the impact of a *persistent* disruption to a specific BMC3 activity? Let us suppose that the disruption begins at time t and ceases later at time τ. The disruption will perturb the nominal Completion State transition probabilities within that interval. The Persistent Disruption Impact on Mission Effectiveness (PDIME) can be determined using the following formula:

$$PDIME_{\phi,t\to\tau} = \sum_{i=1}^{I}\left(P'_{i,t}C_{i,t} - P'_{i,\tau}C_{i,\tau}\right) \qquad (17)$$

where $P'_{i,t}$ and $P'_{i,\tau}$ are the transpose of $P_{i,t}$ and $P_{i,\tau}$, respectively. $P_{i,\tau}$, in turn, is computed by the following equation:

$$P_{i,\tau} = \tilde{\lambda}_{\tau-1}\tilde{\lambda}_{\tau-2}\ldots\tilde{\lambda}_{t}P_{i,t} \qquad i=1,\ldots..I \qquad (18)$$

where $\tilde{\lambda}_{\tau-1}, \tilde{\lambda}_{\tau-2}, \ldots, \tilde{\lambda}_{t}$ are the perturbed Completion State transition probability matrices that result from the disruption to activity ϕ. These perturbed matrices can be estimated for off-nominal conditions of interest using workflow analysis tools.

SECTION 4
COMPUTATION RESULTS

4.1 THE BMC3 WORKFLOW FOR A MISSILE DEFENSE SYSTEM

We illustrate the sensitivity measures derived here for a Ballistic Missile Defense (BMD) system. The objective of this system is to detect missiles and objects released from them; obtain accurate tracks on the objects; discriminate Re-entry Vehicles (RVs) from decoys and other objects; assign weapons to RVs; and provide guidance updates to weapons in-flight. Every object detected by the system corresponds to a 'task' in the BMC3 workflow, but the key task that concerns us is 'RV prosecution.' Some tasks correspond to objects that are not RVs, and for them "task completion" occurs when the BMC3 system correctly identifies them, and launches no weapons against them. The remaining tasks in this workflow correspond to RVs, and for them task completion means the BMC3 successfully destroys the warhead before it strikes an important asset on the ground. Mission Effectiveness, therefore, is the number of RVs successfully destroyed before impact.

The BMC3 system performs 11 primary activities:

1. Detection determines which objects were seen by each sensor during the last sensor scan, and assigns the objects to battlespace sectors;
2. Multi-Sensor Correlation correlates sensor reports and assembles sector tracks;
3. Multi-Sector Data Fusion fuses sector tracks to assemble system tracks on objects;
4. Discrimination classifies the lethality of tracked objects and determines whether the object is eligible for intercept;
5. Battle Planning allocates weapon resources and selects the engagement strategy;
6. Weapon Assignment assigns interceptors to targets placed in the queue awaiting assignment;
7. IFTU Tasking directs communication elements to provide in-flight target updates (IFTUs) to interceptors in flight;
8. Sensor Tasking directs sensors to provide tracking and discrimination support for IFTU generation;

9. Kill Observation Assignment directs sensors to observe anticipated intercept events;
10. Sensor Kill Observation observes a completed interceptor/target engagement and reports impact phenomenology; and
11. Kill Assessment determines whether a target has been engaged successfully, and returns to Weapon Assignment targets that have not been successfully engaged.

Figure 1 illustrates a simplified depiction of the workflow processing for this BMC3 system. The circles correspond to activities, the arcs correspond to potential outcomes, and the flows along these arcs correspond to tasks.

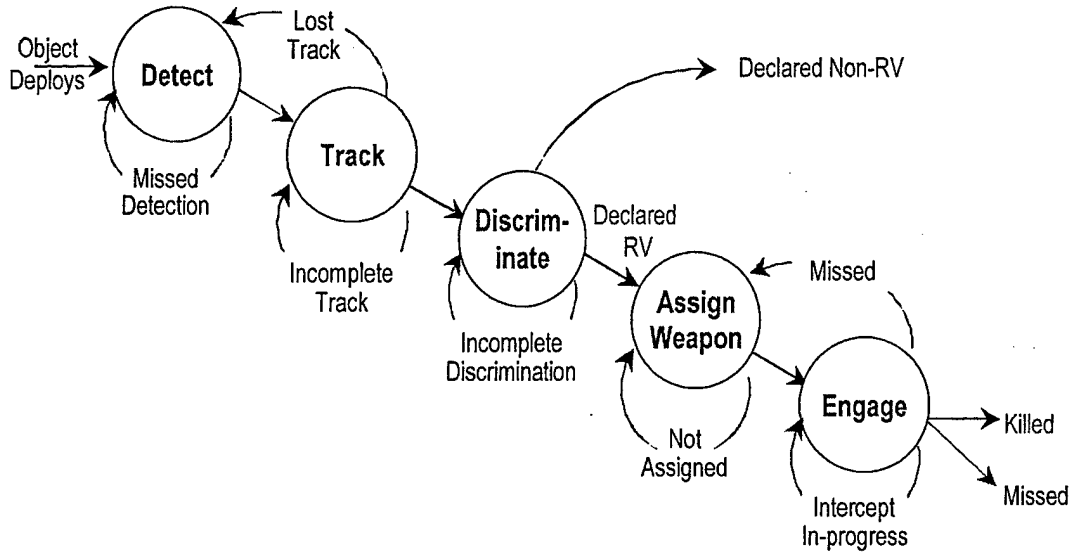

Figure 1. The General Workflow Processing Sequence for the Example BMD System

Workflow analysis identified 68 distinct Completion States for RV prosecution tasks. Most of the activities in this system can operate on several different Completion States, and most Completion States can be acted on concurrently by several activities. The distinction between Completion States lies in the set of activities that can operate on them. Some of these distinctions are slight, however, and several Completion States have nearly identical co-state profiles; we aggregate similar Completion States when we present co-state results.

A Monte-Carlo simulation of this BMD system was retrofitted to record the time when RV prosecution tasks entered and left these 68 Completion States. The simulation was run for 30 Monte-Carlo iterations for a nominal attack scenario, and the state transition probabilities were computed from these runs. In this attack scenario the ballistic missiles launch between 0 and 180 seconds, and the RVs impact their targets near-simultaneously at 1800 seconds.

4.2 Co-State Analysis

We examine here co-state profiles for four aggregate Completion States:

- *Undetected*: the object has been deployed, but the BMC3 system has not detected it.
- *Tracked in 3-D*: the BMC3 system has a high-quality track against the object, but has not yet assigned weapons to the object;
- *Assigned to a Weapon*: the BMC3 system has assigned weapons to the object, but none of the assigned weapons are currently in-flight;
- *Under Engagement*: the BMC3 system has weapons in-flight against the object, but no intercepts have taken place.

Figure 2 presents the co-state profiles for these four states. All profiles peak at different times, each peak corresponding roughly to the time in the battle when the time required to complete the engagement against an RV in that Completion State is comparable to the time remaining to engage the RV before it impacts. For example, it is absolutely essential that the system have an RV in stable 3-D track roughly 300-400 seconds before impact. Discrimination will require roughly 100-200 seconds thereafter, weapon target assignment will require roughly 10-20 seconds, and the interceptor will require roughly 100-200 seconds to fly out to the RV. The co-state for RVs in 3-D track, therefore, is largely negligible at the 1500-second mark (roughly 300 seconds before impact), and peaks at the 1200-second mark.

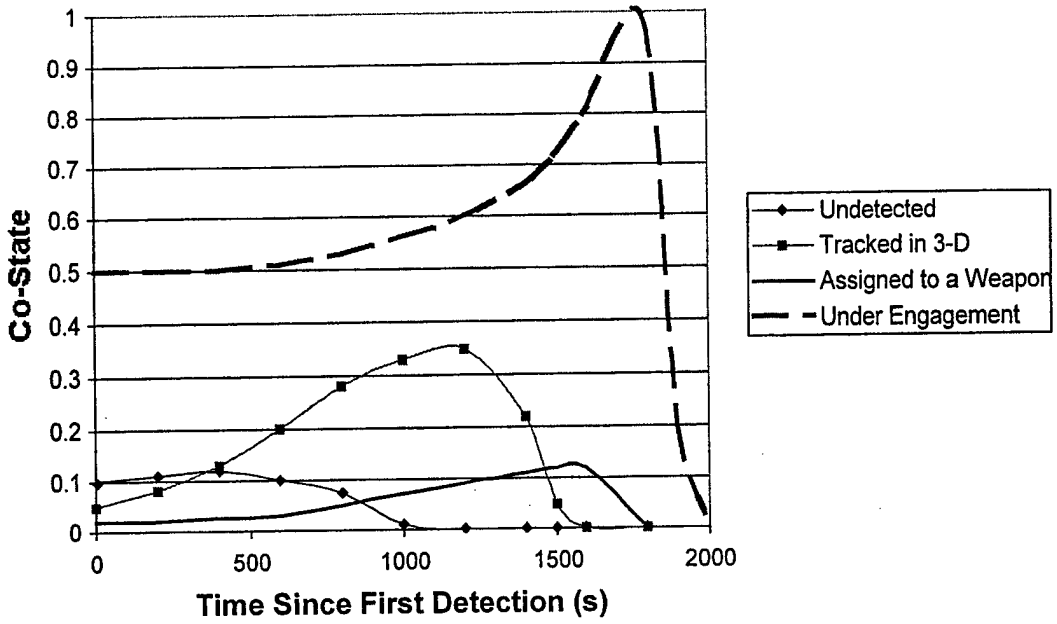

Figure 2. Co-state Profiles for Four Aggregate Completion States

Figure 2 also illustrates another interesting behavior of the co-state: the decline following the peak is sharpest for more advanced completion states. Compare the profiles for the *Undetected* and *Under Engagement* Completion States. The co-state for the first is largely flat, with a modest peak early in the battle. The BMC3 system has several ways to 'recover' the engagement timeline for RVs that are detected after the peaking time; these include using lower lethality thresholds in the Discrimination activity and assigning the target to a weapon with a short time of flight. By contrast, the co-state for the Under Engagement Completion State peaks late in the battle, and declines very rapidly after the peak. Interceptors are flying as fast as they can to RVs in that Completion State, and the BMC3 system simply has no way to recover the engagement if the intercept does not occur before RVs reach their targets.

We comment here in passing on the curious value of the *Under Engagement* co-state early in the battle. This is the penultimate Completion State, and the abnormally large value of the co-state early on is a boundary condition effect. The peak value is correct, however, and reflects the system's weapon-target assignment strategy. The system generally launches a salvo of 3 interceptors against each surviving RV as

the battle draws to a close. Each interceptor has a kill probability of 0.8, and if we assume intercept events are independent, then the cumulative kill probability is 0.992. In short, the system can expect, on average, to obtain $99/100^{ths}$ of the RV value if it is able to complete the salvo engagement before the RV strikes its target.

4.3 IDIME Analysis

Figure 3 presents IDIME profiles for three BMC3 activities: Detection, Weapon Assignment, and Kill Assessment. The IDIME profiles for Weapon Assignment and Kill Assessment have several peaks, and these identify distinct epochs in the battle. The IDIME profile for Weapon Assignment first peaks (modestly) roughly 300 seconds into the battle: this corresponds to the first time that a noticeable number of RVs are eligible for Weapon Assignment. This peak occurs early in the battle when co-state values for Completion States in the Potential Work List are small. The Kill Assessment activity has its first peak roughly 550-600 seconds into the battle; this corresponds to the time when intercepts from the first wave of weapon assignments have completed and are eligible for kill assessment.

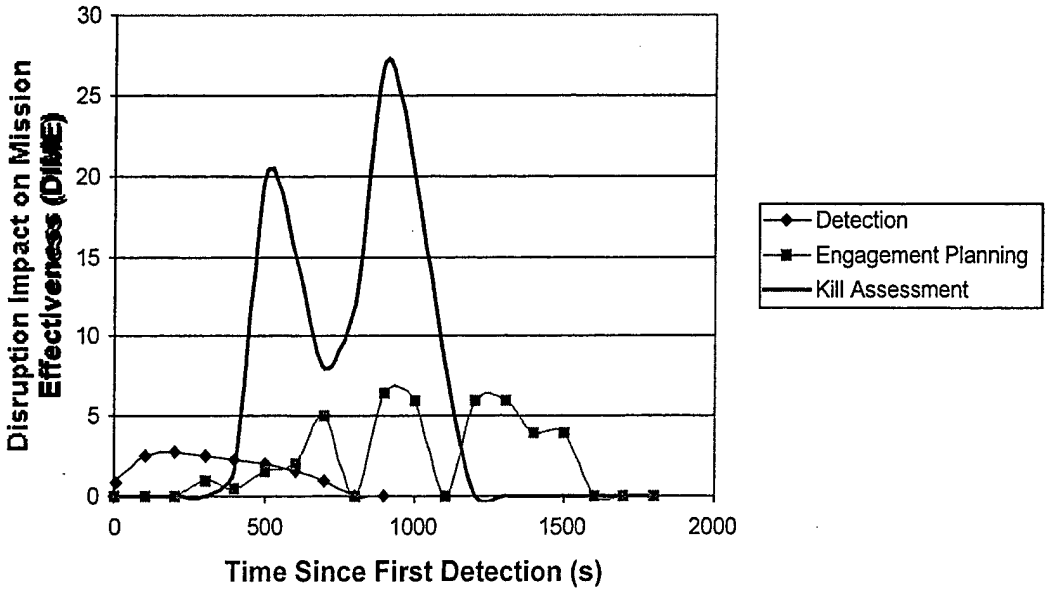

Figure 3. IDIME Profiles for Three BMC3 Activities

The next epoch occurs when Weapon Assignment makes a second round of weapon assignments, roughly 600 seconds into the battle. The IDIME profile for the Weapon Assignment activity peaks at that time, and the IDIME profile for the Kill Assessment follows suit with a peak roughly 300-400 seconds later when intercepts from those assignments have completed. There is a third peak in the IDIME profile for Weapon Assignment roughly 1000 seconds into the battle, corresponding to a small number of RVs that had escaped detection up to that point.

The last epoch occurs when Weapon Assignment makes a final round of weapon assignments, roughly 1200-1500 seconds into the battle. There are actually very few RVs that can be engaged at this point, but the IDIME profile peaks because the co-state values are significant for Completion States in the Potential Work List. There is no further peak in the IDIME profile for the Kill Assessment activity in this final epoch, despite active engagements against RVs, simply because the system has no time remaining to re-engage RVs that survive engagements during this epoch; Kill Assessment has no effect during this epoch.

4.4 PDIME Analysis

Here we evaluate how well the PDIME metric presented in Section 3.4 predicts the actual impact of a persistent disruption to a specific BMC3 activity. The activity of interest is Discrimination, and the disruption simulated retards that activity's processing rate throughout the entire missile attack. We simulated different disruption conditions by retarding this activity's processing rate parametrically; 30 Monte-Carlo iterations were run for each disruption condition. The cost-to-go and approximate co-state metrics were computed for the nominal condition, and perturbed state transition probability matrices were computed for each of the disruption conditions. The PDIME metric was then computed for each disruption condition, per Equations 17 and 18, and compared to the actual average Mission Effectiveness computed for each condition.

We computed the perturbed state transition probability matrices using two different approaches. The

first approach computed the matrices using the full state transition statistics collected for each condition. These 'fully perturbed' matrices capture all impacts on task completion rates that arise when a single activity is disrupted. These impacts can include changes the BMC3 system makes to workflow processing elsewhere in order to compensate for the disrupted activity. The second approach used hybrid matrices starting with the transition matrices for the nominal condition, and replacing the columns corresponding to Completion States in the Discrimination Potential Work List with the new transition probabilities computed for each off-nominal condition. These hybrid matrices presume that the impact on task completion rates is confined only to Completion States in the Potential Work List for the disrupted function; they ignore compensating actions the BMC3 system might take to respond to the disruption.

Figures 4 and 5 compare the mission impacts predicted using the PDIME metric with the actual mission impacts using fully-perturbed and hybrid state transition probability matrices, respectively. The extremely close agreement in Figure 4 between the predicted and actual mission impacts indicates that the co-state and PDIME metrics accurately characterize the impact of a disruption to BMC3 workflow processing.

The agreement between predicted and actual mission impacts is not as good, however, when we use hybrid matrices (Figure 5). The predicted Mission Effectiveness consistently underestimates the actual effectiveness in the off-nominal conditions. This happens because the hybrid matrices ignore compensating actions that the BMC3 system can take to respond to a disruption. In this missile defense system, the BMC3 can compensate for delays in completing Discrimination by short-circuiting downstream workflow activities. Nevertheless, the PDIME metric correctly predicts the trend in the impact on Mission Effectiveness, and the prediction is good in the neighborhood of the nominal condition.

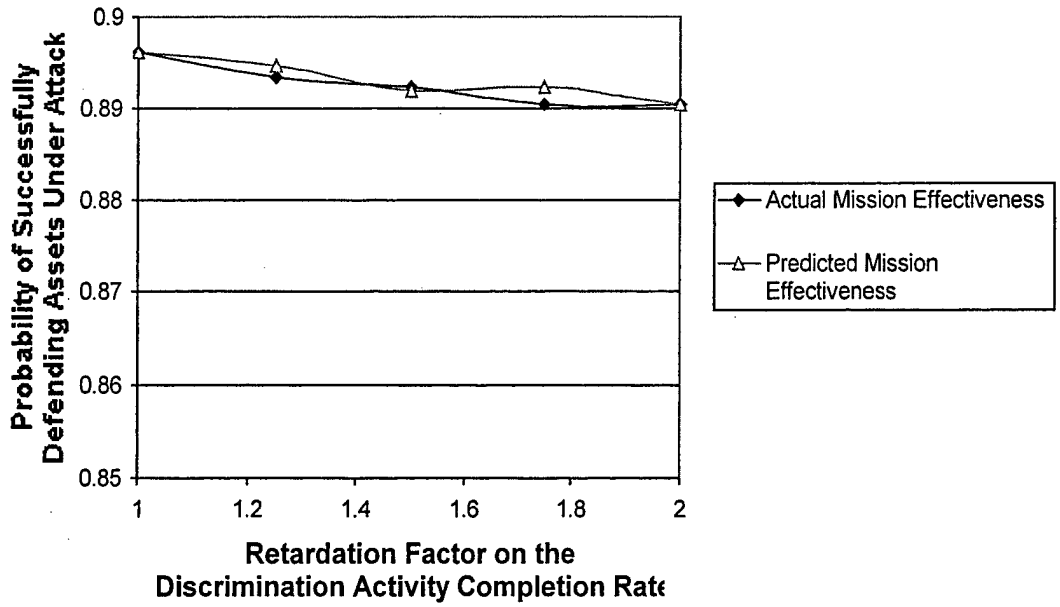

Figure 4. The Agreement Between Actual and Predicted Mission Effectiveness Using Fully-Perturbed State Transition Probability Matrices to Compute PDIME

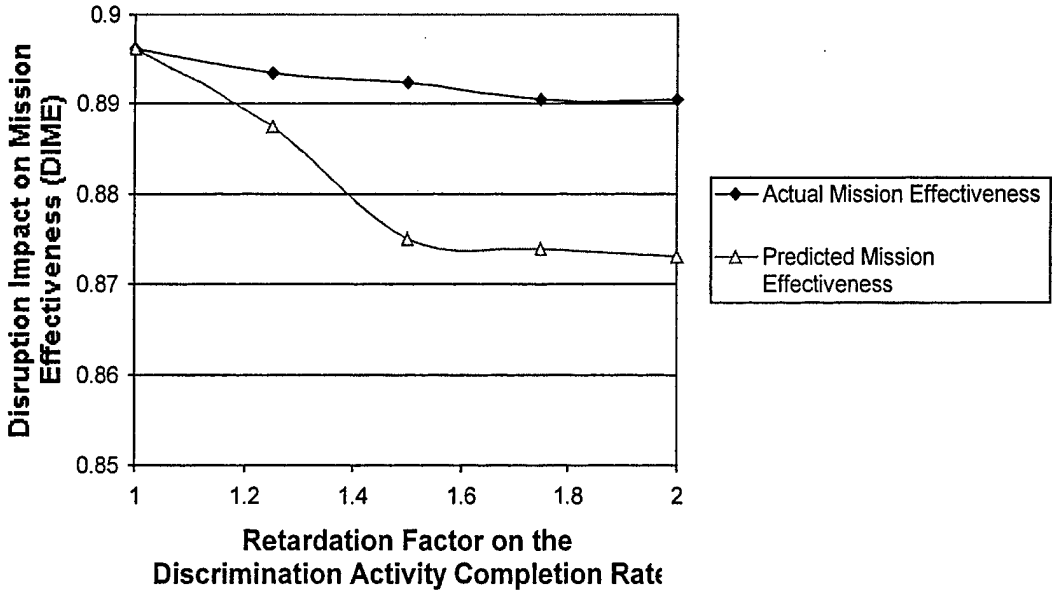

Figure 5. The Agreement Between Actual and Predicted Mission Effectiveness Using Hybrid State Transition Probability Matrices to Compute PDIME

SECTION 5
CLOSING REMARKS AND FUTURE WORK

Measures to safeguard or respond to a cyber attack against a BMC3 system will invariably disrupt the processing flow within that system. We would like to predict the impacts of those disruptions beforehand and select information assurance measures that minimize the disruptions, especially to key BMC3 functions.

In our feasibility study for EBCOTE, we developed an analysis method based on perturbation analysis. The method approximates the nominal BMC3 workflow processing using a Markov model, and computes important sensitivity metrics from Optimal Control Theory, most notably *cost-to-go*, and *co-state*. The key parameters required by this analysis method are Completion State transition probabilities, and these can be computed using data that is regularly collected by advanced workflow management systems.

The logical step from here is to demonstrate the analysis method in a real-time BMC3 system. We have such a system in mind: a prototype center for prosecuting time-critical targets (TCTs). This prototype, the Software Integration Facility for TCTs (SWIFT), is a laboratory established by the Air Force Electronic Systems Center at Hanscom Air Force Base in Massachusetts. The laboratory is the staging ground for integrating new mission applications into existing Air Force tactical BMC3 systems. The laboratory also assembles prototype systems for Joint and Coalition exercises. Our objective would be to install a workflow management system in the SWIFT to collect workflow completion statistics for TCT prosecution missions, and demonstrate the perturbation analysis presented here.

REFERENCES

[1] Workflow Management Coalition, *Workflow Management Coalition Terminology and Glossary*, Document WFMC-TC-1011, Brussels, Belgium, June 1996.

[2] W.M.P. van der Alst, "Petri-net-based Workflow Management Software," *Proceedings of the NFS Workshop on Workflow and Process Automation in Information Systems*, A. Sheth, Ed., pp 114-118, Athens, GA, May 1996.

[3] C.A. Ellis, and G.J. Nutt, "Modelling and Enactment of Workflow Systems," *Application and Theory of Petri Nets 1993*, M. Marsan, Ed., pp 1-16, Springer-Verlag, Berlin, 1993.

[4] R. Ardhaldjian, and M. Fahner, "Using Simulation in the Business Process Reengineering Effort," *Industrial Engineering*, pp 60-61, July 1994.

[5] W.M.P. van der Alst, "The Application of Petri Nets to Workflow Management," *Journal of Circuits, Systems, and Computers*, pp 21-66, Vol. 8, No. 1, 1998.

[6] D.P. Bertsekas, *Dynamic Programming and Optimal Control*, Athena Scientific, Belmont, MA, 1995.

DISTRIBUTION LIST

addresses	number of copies
PETER J. ROCCI, JR. AFRL/IFTD 525 BROOKS ROAD ROME, NY 13441-4505	5
ALPHATECH, INC. 50 MALL ROAD BURLINGTON, MA 01803-4562	5
AFRL/IFOIL TECHNICAL LIBRARY 26 ELECTRONIC PKY ROME NY 13441-4514	1
ATTENTION: DTIC-OCC DEFENSE TECHNICAL INFO CENTER 8725 JOHN J. KINGMAN ROAD, STE 0944 FT. BELVOIR, VA 22060-6218	1
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY 3701 NORTH FAIRFAX DRIVE ARLINGTON VA 22203-1714	1
ATTN: NAN PFRIMMER IIT RESEARCH INSTITUTE 201 MILL ST. ROME, NY 13440	1
AFIT ACADEMIC LIBRARY AFIT/LDR, 2950 P.STREET AREA B, BLDG 642 WRIGHT-PATTERSON AFB OH 45433-7765	1
AFRL/HESC-TDC 2698 G STREET, BLDG 190 WRIGHT-PATTERSON AFB OH 45433-7604	1

ATTN: SMDC IM PL
US ARMY SPACE & MISSILE DEF CMD
P.O. BOX 1500
HUNTSVILLE AL 35807-3801

1

COMMANDER, CODE 4TL000D
TECHNICAL LIBRARY, NAWC-WD
1 ADMINISTRATION CIRCLE
CHINA LAKE CA 93555-6100

1

CDR, US ARMY AVIATION & MISSILE CMD
REDSTONE SCIENTIFIC INFORMATION CTR
ATTN: AMSAM-RD-OB-R, (DOCUMENTS)
REDSTONE ARSENAL AL 35898-5000

2

REPORT LIBRARY
MS P364
LOS ALAMOS NATIONAL LABORATORY
LOS ALAMOS NM 87545

1

ATTN: D'BORAH HART
AVIATION BRANCH SVC 122.10
FOB10A, RM 931
800 INDEPENDENCE AVE, SW
WASHINGTON DC 20591

1

AFIWC/MSY
102 HALL BLVD, STE 315
SAN ANTONIO TX 78243-7016

1

ATTN: KAROLA M. YOURISON
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE
PITTSBURGH PA 15213

1

USAF/AIR FORCE RESEARCH LABORATORY
AFRL/VSOSA(LIBRARY-BLDG 1103)
5 WRIGHT DRIVE
HANSCOM AFB MA 01731-3004

1

ATTN: EILEEN LADUKE/D460
MITRE CORPORATION
202 BURLINGTON RD
BEDFORD MA 01730

1

OUSD(P)/DTSA/DUTD 1
ATTN: PATRICK G. SULLIVAN, JR.
400 ARMY NAVY DRIVE
SUITE 300
ARLINGTON VA 22202

AFRL/IFT 1
525 BROOKS ROAD
ROME, NY 13441-4505

AFRL/IFTM 1
525 BROOKS ROAD
ROME, NY 13441-4505

MISSION
OF
AFRL/INFORMATION DIRECTORATE (IF)

The advancement and application of Information Systems Science and Technology to meet Air Force unique requirements for Information Dominance and its transition to aerospace systems to meet Air Force needs.